UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/394,143	09/10/1999	PAUL CHARLES TURGEON	044624-15-NP	3795

20350 7590 03/12/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
HEWITT II, CALVIN L	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 03/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 30

Application Number: 09/394,143
Filing Date: September 10, 1999
Appellant(s): TURGEON, PAUL CHARLES

MAILED

MAR 12 2004

GROUP 3600

Patrick M. Boucher, Reg. No. 44,037
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 23 December 2003.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims 1-4 and 9-25 and claims 5-8 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

6,173,269	SOLOKL et al.	1-2001
5,771,291	NEWTON et al.	6-1998
5,371,797	BOCINSKY, Jr.	12-1994

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Response to Amendment/Argument

The Applicant has amended independent claims 1 and 17 to include the language, "at least some of said financial accounts being maintained at different ones of said financial institutions". However, this limitation has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Claim Rejections - 35 USC § 103

Claims 1-4, 9-12, 17-23, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Newton et al., U.S. Patent No. 5,771,291 in view of Solokl et al., U.S. Patent No. 6,173,269.

As per claims 1-4, 9-12, 17-23, and 25, Solokl et al. teach a system for providing financial resources over a network comprising: a network access device with a browser for interfacing with a public network (figure 1; column 4, lines 13-29) that is connected to an authentication processor over the public network (figure 1; column 4, lines 13-29), the processor in turn connected to a financial institution over a private network and determining access to a user financial account using said private network (figure 2). Solokl et al. teach a user logging onto an account (figure 2; column 7, lines 65-66). To one of ordinary skill, it would have been obvious to have a user provide a first identifier, such as a user name or ID, in order to login. Along with the login procedure, Solokl et al. also teach transferring an authentication parameter to an authentication processor. Solokl et al. do not specifically recite a portable storage medium with encrypted and unencrypted information. Newton et al. teach a system for authenticating users who desire to access remote resources using a network access device that includes a programmable controller for executing code and a memory for interfacing with a public network (figure 1; column 3, lines 17-35) comprising a computer readable portable storage medium (e.g. CD-ROM) having

encrypted and unencrypted information (column 6, lines 33-38; column 7, lines 45-55). Newton et al. teach an authentication processor, such as a decryption processor connected to the public network (column 7, lines 45-55) for decrypting encrypted information to determine access to remote resources (column 7, lines 53-61). Newton et al. also teach a computer host connected to the network access device over the public network that transfers an active module to the network access device (column 6, lines 10-15; column 7, lines 50-53) that demands a user provide an identifier such as a password or user ID in order to access a network (column 6, lines 10-15). Therefore, it would have been obvious to one of ordinary skill to combine the systems of Solokl et al. and Newton et al. in order to improve network security by allowing users to enter longer, and hence more secure, identification codes and providing an efficient means for entering the code ('291, figure 1; column 8, lines 20-29).

Claims 5-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Newton et al., U.S. Patent No. 5,771,291 and Solokl et al., U.S. Patent No. 6,173,269 as applied to claim 4 above, and further in view of Bocinsky Jr., U.S. Patent No. 5,371,797.

As per claims 5-8, Solokl et al. teach a user logging onto or gaining entrance to multiple networks (figure 2). Solokl et al. also teach displaying data to a user upon successful authentication (figure 2). Newton et al. teach a secure

method for logging onto a network using authentication/identifier data such as encrypted identification keys, passwords and IDs (column 6, lines 10-15; column 7, lines 45-61). Newton et al. also teach that a host computer has access to a database containing encryption and identification keys that are to be stored on a CD-ROM (column 4, lines 50-52). However, neither Solokl et al. nor Newton et al. specifically recite re-encrypting identifiers. Bocinsky Jr. teaches a system for passing financial data across multiple networks, using a network switch to route data, for securing electronic transactions comprising decrypting an identifier and re-encrypting the identifier prior to sending the identifier across another network (figure 1; column 8, lines 19-25; column/line 9/54-10/41; column 13, lines 30-55). Bocinsky Jr. also teaches financial data as an identifier for determining access to a financial account (column/line 1/15-2/60; column 14, lines 12-20) and a financial institution generating a code reflecting whether or not access has been approved, and transferring the code to a decryption processor (figure 2; column 13, lines 30-55). Regarding the production of the portable storage medium, it would have been obvious to one of ordinary skill to manufacture the CD-ROM using any facility that creates CD-ROMs or other portable storage mediums for storing encrypted information, using an encryption module, and unencrypted information ('291, column 7, lines 45-50). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Solokl et al., Newton et al.,

and Bocinsky Jr. in order to provide a more secure system by encrypting sensitive data as it travels across vulnerable networks.

Claims 14-16 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Newton et al., U.S. Patent No. 5,771,291 and Solokl et al., U.S. Patent No. 6,173,269 as applied to claims 12 and 23 above, and further in view of Campbell U.S. Patent No. 4,259,720.

As per claims 14-16 and 24, Solokl et al. teach a user logging onto or gaining entrance to multiple networks and stored identifiers that pertain to customers and financial institutions, such as PINs and Bank IDs (figure 2). Solokl et al. also teach displaying data to a user upon successful authentication (figure 2). Newton et al. teach a secure method for logging onto a network using authentication/identifier data such as encrypted identification keys, passwords and IDs (column 6, lines 10-15; column 7, lines 45-61). Newton et al. also teach that a host computer has access to a database containing encryption and identification keys that are to be stored on a CD-ROM (column 4, lines 50-52). However, neither Solokl et al. nor Newton et al. specifically recite storing encrypted data at the producer of a portable storage medium that maintains encrypted and unencrypted data. Campbell teaches storing secret identification data in encrypted form (abstract). Regarding the production of the portable storage medium, it would have been obvious to one of ordinary skill to

manufacture the CD-ROM using any facility that creates CD-ROMs or other portable storage mediums for storing encrypted information, using an encryption module, and unencrypted information ('291, column 7, lines 45-50; 720, column 3, lines 35-64). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Solokl et al., Newton et al. and Campbell in order to prevent unauthorized access of the stored secret identification codes ('291, abstract; '720, column 1, lines 32-50).

(11) Response to Argument

Group 1- claims 1-4 and 9-25

The question of whether or not the Examiner has factually supported a prima facie case of obviousness rises and falls with the weight given to a claim's preamble. Specifically, whether limitations from a claim's preamble propagate throughout the claim. The Appellant contends that the preamble "language is 'necessary to give life, meaning and vitality' to the limitations in the body of the claim that express applicability across a plurality of financial institutions" (Appeal Brief, page 6, lines 10-13, second footnote, *Pitney Bowes, Inc v. Hewlett-Packard Co.*, 51 USPQ2d 1161, 1165-66 (Fed. Cir.1999)). The Examiner respectfully disagrees.

The preamble of claim 1 is as follows:

A system for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of *financial institutions* maintaining respective *financial accounts for said plurality of customers, at least some of said financial accounts maintained at different ones of said financial institutions*...

Note, the preamble requires only that *at least some* of the accounts be maintained at different financial institutions. Therefore, there are other accounts that are not. The body of claim 1 only refers to accessing or determining access to "said each customer's financial account", "information pertaining to said each customer's financial account" and a financial institution responsible for maintaining "said each customer's financial account". Hence, the claim is broad enough to read on accounts that are not maintained at different financial institutions. Further, the body of the claim does not refer back specifically to those accounts that are maintained at different ones of said financial institutions. And, according to (*Pitney Bowes, Inc v. Hewlett-Packard Co.*, 51 USPQ2d 1161, 1165-66 (Fed. Cir.1999))

if, however, the body of the claim fully and intrinsically sets forth the complete invention, including all of its limitations, and the preamble offers no distinct definition of any of the claimed invention's limitations, but rather merely states, for example, the purpose or intended use of the invention, then the preamble is of no significance to claim construction because it cannot be said to constitute or explain a claim limitation.

Nonetheless, this feature is taught by Solokl et al.. The phrase, "plurality of *financial institutions* maintaining respective *financial accounts for said plurality of*

customers, at least some of said financial accounts maintained at different ones of said financial institutions..." is equivalent to a limitation specifying that there are at least two institutions. The Appellant admits to such by characterizing the invention as merely being applicable across a plurality of institutions (Appeal Brief, page 6, lines 3-5). Solokl et al. teach a system where a parent is able to create a financial account for a child and place restrictions on the use of said account ('269, column/line 3/60-4/30; column/line 5/55-6/15). Specifically, purchases are made using either VISA or MasterCard (figure 1, items 24-28, 30 and 31; column 6, lines 40-50) or with a partner bank and an associated financial institution (figure 1, items 18, 20 and 28; column 5, lines 47-55). Therefore, to one of ordinary skill, the system of Solokl et al. operates across a plurality of institutions, partner banks and "financial institution" or a credit card company (e.g. VISA or MasterCard). However, *In re Delisle*, (160USPQ 806 (CCPA 1969)) and *In re Shepard* (138 USPQ 148 (CCPA 1963)) are clear and it would have been obvious to one of ordinary skill in credit cards and banking that different users can have accounts in different banks (JPMorgan-Chase, Wachovia, Citibank) and that individual or different users would have different or multiple credit cards (AMEX, BankOne, VISA). Therefore, to one of ordinary skill the system of Solokl et al. would operate across these different financial entities (VISA, Citibank...etc.).

In an attempt to clarify the Appellant's position, the Appellant refers to "debit transactions" and "customers accessing accounts at those different institutions" (Appeal Brief, page 6, lines 10-13). However, these limitations are not found in the claims (1 and 17).

The Appellant also asserts that there is no reason to combine the inventions of Solokl et al. and Newton et al. The Appellant is of the opinion that because the Solokl et al. system requires a "pass phrase" ('269, figure 2) transmitted in the clear it prohibits a combination with Newton et al. Again, the Examiner respectfully disagrees. The Appellant is attempting to mischaracterize the Examiner's motivation to combine the two teachings. In the Final Rejection (paper 27, provided above, page 3, section 4, lines 10-15), the Examiner specifically points out that users of the Solokl et al. system are required to login into an account in order to initiate a transaction (figure 2; column 7, lines 65-66). Note, this step (figure 2, 40) is prior to and distinct from the transmission of a pass phrase (figure 2, 44). To one of ordinary skill in network security or computer security, a user name or identifier can be used to log into a computer. Solokl et al. do not specifically disclose how this is "logon procedure" is performed. Newton et al. provide such a method and one that increases the overall security of the system by allowing users to enter "ultra-long" user identification codes using a portable medium, such as a CD-ROM with unencrypted and encrypted information stored thereupon to log on to a computer

network ('291, figure 1; column 3, lines 17-35; column 6, lines 10-15 and 33-38; column 7, lines 45-55).

The Appellant also invokes In re Lee (61 USPQ2d 1430, 1433 (Fed Cir. 2002)). However, the In re Lee analysis is not applicable to the current case. The Examiner has "not rejected the need for 'any specific hint or suggestion in a particular reference'", nor has the Examiner suggested "that common knowledge and common sense are a substitute for evidence". To the contrary, the Examiner considered the full teachings of Solokl et al. and saw that by combining it with Newton et al. a beneficial result was achieved. More specifically, the Newton et al. method for securely logging onto a network adds another layer of security by making it more difficult for an intruder to improperly obtain the login parameters (e.g. id, password) of a valid user ('291, column 1, lines 9-20) (The strongest rationale for combining references is a recognition, expressly or impliedly in the prior art or drawn from a convincing line of reasoning based on established scientific principles or legal precedent, that some advantage or expected beneficial result would have been produced by their combination. *In re Sernaker*, 702 F.2d 989, 994-95, 217 USPQ 1, 5-6 (Fed. Cir. 1983)).

Group 2- claims 5-8

In order to understand the limitation of claim 5, the Examiner referred to the Appellant's disclosure. Specifically, the Appellant teaches encrypting a "blob"

that contains a "first" identifier such as, a cardholder name and address, decrypting the "blob" (i.e. the identifier/cardholder name and address) at a network processor and then forwarding a message that contains approval/denial codes, trace information and information necessary to populate a shipping address screen (Specification, page/line 5/23-6/18). Note, the only "identifier" found in this message is the "card information". The Appellant explicitly states that card information is never available except in encrypted form (Specification, page 6, lines 13-18). To one of ordinary skill, a cardholder name and address (i.e. first identifier) is such information, therefore when the network processor transmits the message, according to the Appellant the card information (i.e. cardholder name and address). The Appellant also discloses an encrypted PIN being transferred to a network processor and the network processor decrypting then re-encrypting the PIN prior to the PIN being sent to the network switch (Specification, page 7, lines 5-7; page 13, lines 12-22). In either case, claim 5, in light of the Appellant's disclosure teaches the first identifier (i.e. card information, PIN) coinciding with the second identifier. It is important to point out that although the Appellant discloses SSL, in the context of the encrypted identifier, the Appellant's encrypting and re-encrypting of the identifier is performed outside of SSL, because the identifiers are encrypted prior to transmission using SSL and the re-encryption is performed by the network processor using a method other than SSL (Specification, page 11, lines 15-25; page 13, lines 12-15). Further,

claims 4 and 5 do not prevent this scenario as the claims are absent language that specifically distinguishes a first identifier being distinct from a second identifier. Hence, the Bocinsky Jr. reference teaches the limitations of claim 5, as the system discloses an ATM, transferring an encrypted identifier to a first processor, the first processor decrypting the encrypted identifier and then re-encrypting the identifier for transmission to a second processor ('797, column 9, lines 35-66).

(12) Conclusion

Appellant's arguments are not persuasive. In order to distinguish claims 1 and 17 from the prior art, the Appellant relies on limitations not found in the body of the claim. Specifically, the Appellant relies on language from the preamble that fails to give life, meaning and vitality' to the limitations in the body of the claim and/or reads limitations from the Specification into the claims. The Appellant also doesn't consider the implications of the language "at least some", where "at least some" means that there are financial accounts that are not maintained at different financial institutions. Regarding claim 5, the Appellant does not fully appreciate Appellant's own teachings with respect to the steps of transferring identifiers such as a PIN or card information, and the breadth of the claim as it does not exclude the possibility of first and second identifier being one and the same.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Calvin Loyd Hewitt II
March 9, 2004

Conferees
James P. Trammell

John Hayes

GOODWIN PROCTER & HOAR LLP
7 BECKER FARM RD
ROSELAND, NJ 07068